

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-069830
 (43)Date of publication of application : 11.03.1997

(51)Int.CI. H04L 9/14
 G09C 1/00

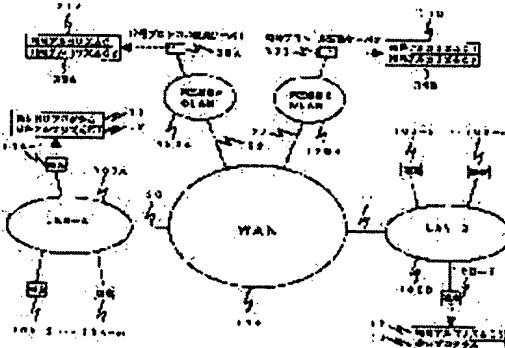
(21)Application number : 07-221928 (71)Applicant : HITACHI LTD
 (22)Date of filing : 30.08.1995 (72)Inventor : NANBA DEN
 TAKARAGI KAZUO
 MIYAZAKI SATOSHI

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:

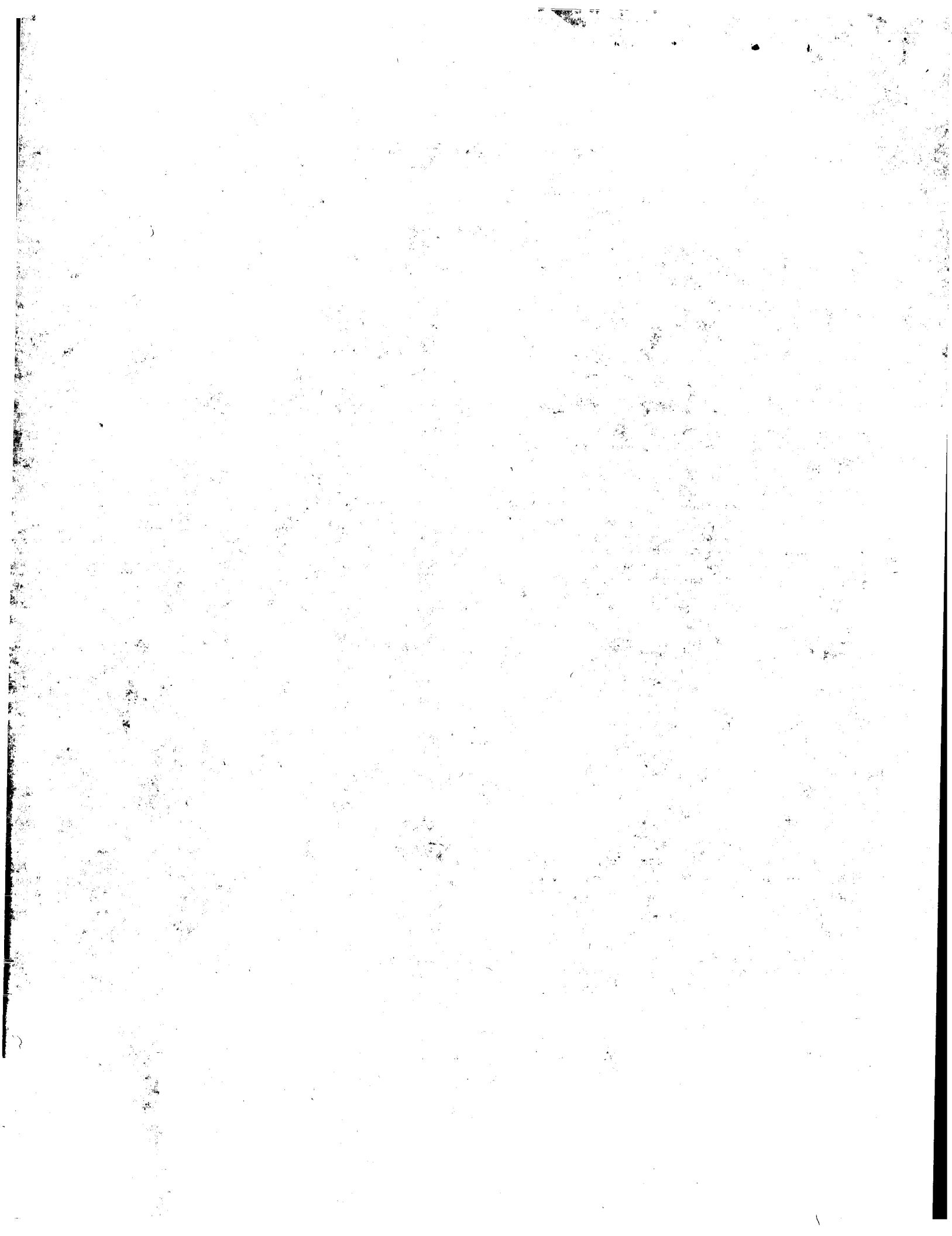
PROBLEM TO BE SOLVED: To safely perform cipher translating processing when performing cipher communication between terminals to use mutually different ciphers.

SOLUTION: When transmitting data to a terminal 10B-1 connected to a LAN-B to use a cipher algorithm C1, a terminal 10A-1 connected to a LAN-A to use a cipher algorithm C1 generates two pieces of data, for which it is difficult to discriminate semantics, from the data to be transmitted. Then, two pieces of generated data are ciphered by using C1 and transmitted while being distributed to two cipher protocol translation servers 1 and 2. The cipher protocol translation servers 1 and 2 decode the data transmitted from the terminal 10A-1 by using C1 while sharing the processing with each other, perform cipher translating processing for reciphering the data by using C2 and then transmit the data to the terminal 10B-1. The terminal 10B-1 decodes the original transmit data from two pieces of data respectively transmitted from the cipher protocol translation servers 1 and 2.



LEGAL STATUS

[Date of request for examination] 07.02.2001
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-69830

(43) 公開日 平成9年(1997)3月11日

(51) Int.Cl.⁹ 認別記号 序内整理番号 F I 技術表示箇所
 H 04 L 9/14 6 6 0 7259-5 J H 04 L 9/00 6 4 1
 G 09 C 1/00 G 09 C 1/00 6 6 0 E

審査請求 未請求 請求項の数11 O.L. (全 22 頁)

(21) 出願番号 特願平7-221928

(22) 出願日 平成7年(1995)8月30日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 究明者 薫波

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立

宝木 和夫

神奈川県

式会社日立製作所システム開発研究所内

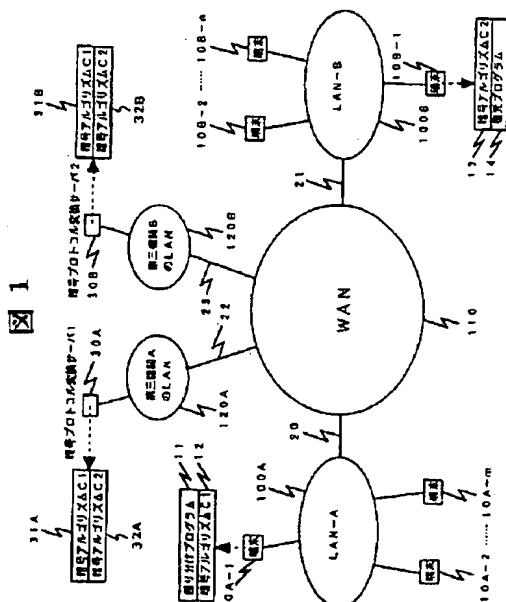
(72) 発明者 宮崎 眞

(54) 【発明の名称】 暗号通信システム

(57) 【要約】

【目的】互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能な暗号通信システムを提供する。

〔構成〕暗号アルゴリズムC1を使用するLAN-Aに接続された端末10A-1は、暗号アルゴリズムC2を使用するLAN-Bに接続された端末10B-1にデータを送信する場合に、送信すべきデータから意味判別困難な2個のデータを生成し、生成した2個のデータを、C1を使用して暗号化した後、2個の暗号プロトコル変換サーバ1、2に振り分けて送信する。暗号プロトコル変換サーバ1、2は、各々分担して、端末10A-1から送信されたデータを、C1を使用して復号化した後、C2を使用して再暗号化する暗号変換処理を行ってから、端末10B-1に送信する。端末10B-1は、暗号プロトコル変換サーバ1、2から各々送信された2個のデータから、元の送信データを復元する。



【特許請求の範囲】

【請求項1】第1の暗号を使用する1個以上の第1種の端末と、上記第1の暗号とは異なる第2の暗号を使用する1個以上の第2種の端末と、上記第1の暗号および上記第2の暗号を使用するn (n ≥ 2) 個の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムであって、

上記第1種の端末は、各々、

上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の暗号プロトコル変換サーバのうちのk (n ≥ k ≥ 2) 個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段と、上記振り分け手段が生成したk個のデータを、上記第1の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の暗号プロトコル変換サーバに送信する送信手段とを有し、

上記n個の暗号プロトコル変換サーバは、各々、

上記第1種の端末のうちのいずれかの端末から送信された1個のデータを、上記第1の暗号で復号化した後、上記第2の暗号で再暗号化する暗号変換手段と、上記暗号変換手段が再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段とを有し、

上記第2種の端末は、各々、

上記k個の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第2の暗号で復号化する復号化手段と、上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段とを有することを特徴とする暗号通信システム。

【請求項2】第1の暗号を使用する1個以上の第1種の端末と、上記第1の暗号とは異なる第2の暗号を使用する1個以上の第2種の端末と、上記第1の暗号および上記第2の暗号を使用するn (n ≥ 2) 個の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムであって、

上記第1種の端末は、各々、

上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の暗号プロトコル変換サーバのうちのk (n ≥ k ≥ 2) 個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段と、上記振り分け手段が生成したk個のデータを、上記第1の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の暗号プロトコル変換サーバに送信する送信手段と、上記k個の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第1の暗号で復号化する復号化手段と、上記復号化手段が復号化したk個のデータから、

元のデータを復元する復元手段とを有し、

上記第2種の端末は、各々、

上記第1種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の暗号プロトコル変換サーバのうちのk (n ≥ k ≥ 2) 個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段と、上記振り分け手段が生成したk個のデータを、上記第2の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の暗号プロトコル変換サーバに送信する送信手段と、上記k個の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第2の暗号で復号化する復号化手段と、上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段とを有し、

上記n個の暗号プロトコル変換サーバは、各々、

上記第1種の端末および上記第2種の端末のうちのいずれかの端末から送信された1個のデータを、上記第1の暗号および上記第2の暗号のうちの、該データに付加されている端末情報が示す送信元の端末が使用する暗号で復号化した後、上記第1の暗号および上記第2の暗号のうちの、該データに付加されている端末情報が示す送信先の端末が使用する暗号で再暗号化する暗号変換手段と、上記暗号変換手段が再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段とを有することを特徴とする暗号通信システム。

【請求項3】第1の暗号を使用する1個以上の第1種の端末と、上記第1の暗号とは異なる第2の暗号を使用する1個以上の第2種の端末と、上記第1の暗号、並びに、上記第1の暗号および上記第2の暗号とは異なる第3の暗号を使用するn個 (n ≥ 2) の第1種の暗号プロトコル変換サーバと、上記第2の暗号および上記第3の暗号を使用し、上記n個の第1種の暗号プロトコルサーバの各々に予め対応付けられたn (n ≥ 2) 個の第2種の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムであって、

上記第1種の端末は、各々、

上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の第1種の暗号プロトコル変換サーバのうちのk (n ≥ k ≥ 2) 個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段と、上記振り分け手段が生成したk個のデータを、上記第1の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の第1種の暗号プロトコル変換サーバに送信する送信手段と、上記k個の第1種の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第1の暗号で復号化する復号化手段と、上記復号化手段が復号化したk個のデータを、

化した k 個のデータから、元のデータを復元する復元手段とを有し。

上記第2種の端末は、各々、

上記第1種の端末のうちのいずれかの端末に送信すべきデータから、上記 n 個の第2種の暗号プロトコル変換サーバのうちの k ($n \geq k \geq 2$) 個の暗号プロトコル変換サーバに振り分けるべき k 個のデータを生成する振り分け手段と、上記振り分け手段が生成した k 個のデータを、上記第2の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化した k 個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記 k 個の第2種の暗号プロトコル変換サーバに送信する送信手段と、上記 k 個の第2種の暗号プロトコル変換サーバの各々から送信された k 個のデータを、上記第2の暗号で復号化する復号化手段と、上記復号化手段が復号化した k 個のデータから、元のデータを復元する復元手段とを有し。

上記 n 個の第1種の暗号プロトコル変換サーバは、各々、

上記第1種の端末のうちのいずれかの端末から送信された1個のデータを、上記第1の暗号で復号化した後、上記第3の暗号で再暗号化し、また、上記 n 個の第2種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバから送信された1個のデータを、上記第3の暗号で復号化した後、上記第1の暗号で再暗号化する暗号変換手段と、上記暗号変換手段が上記第3の暗号で再暗号化した1個のデータを、上記 n 個の第2種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第1の暗号で再暗号化した1個のデータを、該データに付加されている端末情報を示す送信先の端末に送信する送信手段とを有し。

上記 n 個の第2種の暗号プロトコル変換サーバは、各々、

上記第2種の端末のうちのいずれかの端末から送信された1個のデータを、上記第2の暗号で復号化した後、上記第3の暗号で再暗号化し、また、上記 n 個の第1種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバから送信された1個のデータを、上記第3の暗号で復号化した後、上記第2の暗号で再暗号化する暗号変換手段と、上記暗号変換手段が上記第3の暗号で再暗号化した1個のデータを、上記 n 個の第1種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第2の暗号で再暗号化した1個のデータを、該データに付加されている端末情報を示す送信先の端末に送信する送信手段とを有することを特徴とする暗号通信システム。

【請求項4】請求項1、2または3記載の暗号通信システムにおいて、

上記振り分け手段は、データ量が均等で、かつ、生成前のデータのデータ量よりデータ量が小さい k 個のデータを生成することを特徴とする暗号通信システム。

【請求項5】請求項1、2または3記載の暗号通信システムにおいて、

上記振り分け手段は、排他的論理和を取ると生成前のデータと等しくなるような k 個のデータを生成することを特徴とする暗号通信システム。

【請求項6】請求項1、2、3または4記載の暗号通信システムにおいて、

上記振り分け手段は、生成前のデータが一定のデータ量ごとに順次割り当てられた k 個のデータを生成することを特徴とする暗号通信システム。

【請求項7】請求項1～6のいずれか記載の暗号通信システムにおいて、

上記振り分け手段は、生成前のデータを一定のデータ量単位でスクランブルした後、スクランブル後のデータから k 個のデータを生成することを特徴とする暗号通信システム。

20 【請求項8】請求項6または7記載の暗号通信システムにおいて、

上記生成前のデータが文字列を表す場合に、上記一定のデータ量は、1文字分のデータより小さいことを特徴とする暗号通信システム。

【請求項9】請求項1～8のいずれか記載の暗号通信システムにおいて、

上記暗号変換手段は、一定のデータ量ごとに、復号化および再暗号化を行うことを特徴とする暗号通信システム。

30 【請求項10】第1の暗号を使用する1個以上の第1種の端末と、上記第1の暗号とは異なる第2の暗号を使用する1個以上の第2種の端末と、上記第1の暗号および上記第2の暗号を使用し、一方の暗号で暗号化されたデータをもう一方の暗号で暗号化されたデータに暗号変換する n ($n \geq 2$) 個の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムにおいて、上記第1種の端末として用いられる情報処理装置であって、

上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記 n 個の暗号プロトコル変換サーバのうちの k ($n \geq k \geq 2$) 個の暗号プロトコル変換サーバに振り分けるべき k 個のデータを生成する振り分け手段と、上記振り分け手段が生成した k 個のデータを、上記第1の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化した k 個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記 k 個の暗号プロトコル変換サーバに送信する送信手段と、上記 k 個の暗号プロトコル変換サーバの各々から送信された k 個のデータを、上記第1の暗号で復号化する復号化手段と、上記復号化手段が復号化した k 個のデータから、

5
元のデータを復元する復元手段とを有することを特徴とする情報処理装置。

【請求項11】請求項10記載の情報処理装置において、上記振り分け手段は、排他的論理和を取ると生成前のデータと等しくなるようなk個のデータを生成することを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、互いに異なる暗号を使用する端末間で暗号通信を行うことを可能とする暗号通信システムに関するものである。

【0002】

【従来の技術】従来、使用されてきた暗号には、アルゴリズム秘匿型とアルゴリズム公開型があり、前者は、軍隊等で隠密に使用され、後者は、アルゴリズムを一般に公開した上で、銀行等で使用されている。いずれの場合も、1種類の暗号を使用し、閉じたネットワーク内で暗号通信が行われている。

【0003】近年のコンピュータ利用形態のオープン化、マルチベンダ化、インターネット化に伴い、互いに異なるアルゴリズム公開型の暗号を使用する端末が接続されたネットワークを相互接続し、これらのネットワークに各々接続された端末間でも暗号通信を行いたいという要求が生じることが予想される。

【0004】一方、国際標準化機構ISO(International Organization for Standardization)は、1991年に、暗号アルゴリズム登録制度を設立し、暗号アルゴリズムについては1種類に標準化せず、認可登録された複数種類の暗号アルゴリズムを一般に提供していくことを決定した。その結果、将来においても、複数種類の暗号アルゴリズムが地域ごとに使い分けられていく可能性が生じた。日本においても、1994年ISOの暗号アルゴリズム登録制度のJIS(Japanese Industrial Standards)化を行っている。

【0005】互いに異なる暗号を使用する端末が接続されたネットワークを相互接続した場合、これらのネットワークに各々接続された端末間で暗号通信を行うためには、送信元の端末が、送信すべきデータを自身が使用する暗号で暗号化することしかできず、送信先の端末が、自身が使用する暗号で暗号化されたデータしか復号化することができないことから、一旦、送信元の端末が暗号化した送信データを、送信先の端末が使用する暗号で暗号化したデータに変換する必要が生じる。

【0006】このような暗号変換処理に関する公知技術としては、財団法人日本規格協会の調査研究報告書「平成3年度多目的利用ICカード社会における望ましいシステム構築とるべき標準化に関する調査研究報告書」(日機連3標準化-20、平成4年3月、25頁~31頁)において、暗号プロトコル変換装置が開示されてい

る。

【0007】この暗号プロトコル変換装置は、互いに異なる暗号を使用する端末が接続された2個のネットワークを結ぶ通信回線上に設置され、これら2個のネットワークで各々使用されている2種類の暗号アルゴリズム(暗号化アルゴリズムおよび復号化アルゴリズム)を備えるようにしている。

【0008】そして、暗号プロトコル変換装置は、送信元の端末が使用する暗号で暗号化されている送信データを、装置内に備えている、送信元の端末が使用する暗号の復号化アルゴリズムで復号化し、さらに、復号化したデータを、装置内に備えている、送信先の端末が使用する暗号の暗号化アルゴリズムで暗号化するという暗号変換処理を行う。

【0009】

【発明が解決しようとする課題】しかしながら、上述した暗号プロトコル変換装置においては、送信元の端末が暗号化したデータが、一旦、復号化されることから、暗号化される前のデータである「平文」の状態となり、第三者が平文を盗むチャンスが存在してしまい、データの秘匿性が破られる危険性がある。

【0010】そこで、本発明の第1の目的は、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行なうことが可能な暗号通信システムを提供することにある。

【0011】また、上述した公知技術を開示する調査研究報告書においては、暗号プロトコル変換装置が1個のみ設置されている。送信すべきデータのデータ量が多い場合は、暗号プロトコル変換装置が1個のみでは、暗号変換処理を高速に行なうことはできず、暗号変換処理に関するオーバヘッドが大きくなると考えられる。

【0012】将来的には、テラ(1テラ=1ギガ×1000)bpsに及ぶ大容量通信の時代が到来することが予想されており、このような大容量通信の時代には、通信路の高速化が重要な課題である。

【0013】そこで、本発明の第2の目的は、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、高速に行なうことが可能な暗号通信システムを提供することにある。

【0014】さらに、上述した暗号プロトコル変換装置は、各端末が使用する2種類の暗号アルゴリズム(暗号化アルゴリズムおよび復号化アルゴリズム)を備えるようにしているが、これらの端末が各々接続されたネットワークが異なる国に属する場合には、必ずしも実現可能ではない。実際、例えば、米国は、法律により、暗号技術(米国暗号標準DES等)の輸出入を規制している。このような規制が適用された場合、自国に属するネットワークに接続された端末が使用する暗号アルゴリズムを他国内に設置された暗号プロトコル変換装置に備えることができず、暗号通信を行なうことができなくなる。

【0015】そこで、本発明の第3の目的は、互いに異なる暗号を使用する端末が異なる国に属する場合でも、上記第1の目的を達成することが可能な暗号通信システムを提供することにある。

【0016】

【課題を解決するための手段】上記第1の目的を達成するため、本発明においては、互いに異なる暗号を使用する端末間で送受信するデータが、複数の暗号プロトコル変換サーバを経由するようにし、これらの複数の暗号プロトコル変換サーバが分担して上述した暗号変換処理を行うようにしている。そして、複数の暗号プロトコル変換サーバに暗号変換処理を分担させるために、送信元の端末が、送信すべきデータから、複数の暗号プロトコル変換サーバに振り分けるべき複数のデータを生成するようにしている。

【0017】そのために、本発明は、第1の暗号を使用する1個以上の第1種の端末と、上記第1の暗号とは異なる第2の暗号を使用する1個以上の第2種の端末と、上記第1の暗号および上記第2の暗号を使用するn (n ≥ 2) 個の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムを提供しており、上記第1種の端末が、各々、(1) 上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の暗号プロトコル変換サーバのうちのk (n ≥ k ≥ 2) 個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段、(2) 上記振り分け手段が生成したk個のデータを、上記第1の暗号で暗号化する暗号化手段、(3) 上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の暗号プロトコル変換サーバに送信する送信手段、(4) 上記k個の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第1の暗号で復号化する復号化手段、(5) 上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段、を有するようにし、上記第2種の端末が、各々、(1) 上記第1種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の暗号プロトコル変換サーバのうちのk (n ≥ k ≥ 2) 個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段、(2) 上記振り分け手段が生成したk個のデータを、上記第2の暗号で暗号化する暗号化手段、(3) 上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の暗号プロトコル変換サーバに送信する送信手段、(4) 上記k個の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第2の暗号で復号化する復号化手段、(5) 上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段、を有するようにし、上記n個の暗号プロトコル変換サーバが、各々、(1) 上

記第1種の端末および上記第2種の端末のうちのいずれかの端末から送信された1個のデータを、上記第1の暗号および上記第2の暗号のうちの、該データに付加されている端末情報が示す送信元の端末が使用する暗号で復号化した後、上記第1の暗号および上記第2の暗号のうちの、該データに付加されている端末情報が示す送信先の端末が使用する暗号で再暗号化する暗号変換手段、

(2) 上記暗号変換手段が再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段、を有するようにしている。

【0018】例えば、上記振り分け手段は、排他的論理和を取ると生成前のデータと等しくなるようなk個のデータを生成するようにすることができる。このとき、さらに、上記振り分け手段は、生成前のデータを一定のデータ量単位でスクランブルした後、スクランブル後のデータからk個のデータを生成するようにしてもよい。なお、一定のデータ量が、1文字分のデータより小さいデータ量であることが好ましい。

【0019】また、例えば、上記暗号変換手段は、一定のデータ量ごとに、復号化および再暗号化を行うようにすることができる。

【0020】また、上記第2の目的を達成するために、本発明においては、複数の暗号プロトコル変換サーバが分担して暗号変換処理を行うデータ、すなわち、送信元の端末が生成する複数のデータの各々が、元のデータのデータ量よりデータ量が小さいデータであるようにしている。

【0021】すなわち、上記振り分け手段は、データ量が均等で、かつ、生成前のデータのデータ量より小さいk個のデータを生成するようにしている。

【0022】例えば、上記振り分け手段は、生成前のデータが一定のデータ量ごとに順次割り当てられたk個のデータを生成するようにすることができる。このとき、さらに、上記振り分け手段は、生成前のデータを一定のデータ量単位でスクランブルした後、スクランブル後のデータからk個のデータを生成するようにしてもよい。

【0023】また、上記第3の目的を達成するために、本発明においては、互いに異なる暗号を使用する端末が異なる国に属する場合に、これらの国が共通に使用するよう協定した1個の暗号を利用し、これらの端末間で送受信されるデータが、国境を越えるときには、該協定した暗号で暗号化された状態となるようにしている。

【0024】このように、協定した暗号を利用することで、各暗号プロトコル変換サーバは、自身が属する国とは異なる国に属する端末が使用する暗号を使用する必要がなくなり、上記第1の目的を達成するための暗号通信システムを構築することができるようになる。

【0025】そのために、本発明は、第1の暗号を使用する1個以上の第1種の端末と、上記第1の暗号とは異なる第2の暗号を使用する1個以上の第2種の端末と、

上記第1の暗号、並びに、上記第1の暗号および上記第2の暗号とは異なる第3の暗号を使用するn個($n \geq 2$)の第1種の暗号プロトコル変換サーバと、上記第2の暗号および上記第3の暗号を使用し、上記n個の第1種の暗号プロトコルサーバの各々に予め対応付けられたn($n \geq 2$)個の第2種の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムを提供しており、上記第1種の端末が、各々、(1)上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の第1種の暗号プロトコル変換サーバのうちのk($n \geq k \geq 2$)個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段、(2)上記振り分け手段が生成したk個のデータを、上記第1の暗号で暗号化する暗号化手段、(3)上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の第1種の暗号プロトコル変換サーバに送信する送信手段、(4)上記k個の第1種の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第1の暗号で復号化する復号化手段、(5)上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段、を有するようにし、上記第2種の端末が、各々、(1)上記第1種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の第2種の暗号プロトコル変換サーバのうちのk($n \geq k \geq 2$)個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段、(2)上記振り分け手段が生成したk個のデータを、上記第2の暗号で暗号化する暗号化手段、(3)上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の第2種の暗号プロトコル変換サーバに送信する送信手段、(4)上記k個の第2種の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第2の暗号で復号化する復号化手段、(5)上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段、を有するようにし、上記n個の第1種の暗号プロトコル変換サーバが、各々、(1)上記第1種の端末のうちのいずれかの端末から送信された1個のデータを、上記第1の暗号で復号化した後、上記第3の暗号で再暗号化し、また、上記n個の第2種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバから送信された1個のデータを、上記第3の暗号で復号化した後、上記第1の暗号で再暗号化する暗号変換手段、(2)上記暗号変換手段が上記第3の暗号で再暗号化した1個のデータを、上記n個の第2種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第1の暗号で再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信

手段、を有するようにし、上記n個の第2種の暗号プロトコル変換サーバが、各々、(1)上記第2種の端末のうちのいずれかの端末から送信された1個のデータを、上記第2の暗号で復号化した後、上記第3の暗号で再暗号化し、また、上記n個の第1種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバから送信された1個のデータを、上記第3の暗号で復号化した後、上記第2の暗号で再暗号化する暗号変換手段、(2)上記暗号変換手段が上記第3の暗号で再暗号化した1個のデータを、上記n個の第1種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第2の暗号で再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段、を有するようにしている。

【0026】

【作用】本発明の暗号通信システムによれば、送信元の端末において、上記振り分け手段が、送信すべきデータから、平文状態で意味判別困難な複数のデータを生成するようになっていると共に、複数の暗号プロトコル変換サーバが暗号変換処理を分担して行うようになっているので、全ての暗号プロトコル変換サーバから平文状態のデータが盗まれたとしても、複数のデータの生成方法が知られない限り、データの秘匿性は守られることとなり、逆に、複数のデータの生成方法が知られたとしても、全ての暗号プロトコル変換サーバから平文状態のデータが盗まれない化ぎり、データの秘匿性は守られることとなる。

【0027】また、例えば、暗号プロトコル変換サーバにおいて、上記暗号変換手段が、一定のデータ量ごとに暗号変換処理を行うようにすれば、同時に平文状態となるデータの量が、該一定のデータ量のみとなるので、データが平文状態となる時間が短くなり、また、この時間に平文状態のデータが盗まれても、該一定のデータ量のデータのみが判別するだけで済む。

【0028】さらに、送信元の端末において、上記振り分け手段が、送信すべきデータから、該データのデータ量よりデータ量が小さい複数のデータを生成するようすれば、複数の暗号プロトコル変換サーバ間で負荷が分散され、各暗号プロトコル変換サーバが行う暗号変換処理の負荷が軽減される。

【0029】

【実施例】以下、本発明の実施例について図面を参照して説明する。

【0030】図1は本発明の第1の実施例の暗号通信システムの構成図である。

【0031】図1に示した暗号通信システムは、互いに異なる暗号を使用する2個のLAN(Local Area Network)であるLAN-A(100A)、LAN-B(100B)に各々接続されている任意の端末間で、暗号通信

を行うためのものである。

【0032】この暗号通信は、WAN (Wide Area Network) 110、暗号プロトコル変換サーバ1 (30A)、暗号プロトコル変換サーバ2 (30B) を経由して行われる。

【0033】図1に示すように、LAN-A (100A) は、暗号アルゴリズムC1 (12) を備え、これを使用する複数の端末10A-1～10A-mが接続されたローカルエリア・ネットワークであり、LAN-B (100B) は、暗号アルゴリズムC2 (13) を備え、これを使用する複数の端末10B-1～10B-nが接続されたローカルエリア・ネットワークであり、各々、通信回線20、21を介して、WAN110と接続されている。

【0034】また、暗号プロトコル変換サーバ1 (30A) が属する第三機関AのLAN (120A)、および、暗号プロトコル変換サーバ2 (30B) が属する第三機関BのLAN (120B) が、各々、通信回線22、23を介して、WAN110と接続されている。

【0035】以下、LAN-A (100A) に接続された端末10A-1からLAN-B (100B) に接続された端末10B-1に対する暗号通信を例にして、暗号通信システムの動作概要を説明する。

【0036】送信元の端末10A-1は、送信先の端末10B-1に送信すべきデータを、自身が備えている振り分けプログラム11を使用して2個に振り分ける振り分け処理を行う。そして、端末10A-1は、振り分け処理を行った後の方のデータを、自身が備えているアルゴリズムC1 (12) を使用して暗号化し、WAN110を経由して、暗号プロトコル変換サーバ1 (30A) に送信する。また、もう一方のデータを、自身が備えているアルゴリズムC1 (12) を使用して暗号化し、WAN110を経由して、暗号プロトコル変換サーバ2 (30B) に送信する。

【0037】暗号プロトコル変換サーバ1 (30A)、暗号プロトコル変換サーバ2 (30B) は、各々、端末10A-1から送信されたデータを、自身が備えているアルゴリズムC1 (31A、31B) を使用して復号化し、さらに、受信先の端末10B-1が備えているアルゴリズムC2 (13) と同じアルゴリズムC2 (32A、32B) を使用して再暗号化するという暗号変換処理を行う。そして、暗号プロトコル変換サーバ1 (30A)、暗号プロトコル変換サーバ2 (30B) は、各々、暗号変換処理を行った後のデータを、WAN110を介して受信先の端末10B-1に送信する。

【0038】受信先の端末10B-1は、暗号プロトコル変換サーバ1 (30A) から送信されたデータ、および、暗号プロトコル変換サーバ2 (30B) から送信されたデータを、各々、自身が備えているアルゴリズムC2 (13) を使用して復号化し、さらに、復号化した2

個のデータを、自身が備えている復元プログラム14を使用して、元のデータに復元する。

【0039】本実施例は、振り分けプログラム11による振り分け方法を工夫することで、従来は暗号変換処理時に平文状態となっていたデータの秘匿性を高めることを特徴とするものである。以下、振り分け方法の具体例を含め、暗号通信システムに関するさらに詳細な説明を行う。

【0040】な、以下の説明においては、LAN-A (100A) とLAN-B (100B) とが、互いに異なる同ブロック長のブロック型慣用暗号を使用している場合に、LAN-A (100A) に接続された端末10A-1からLAN-B (100B) に接続された端末10B-1に対する暗号通信を例にして、暗号通信システムの詳細な動作について説明する。

【0041】まず、送信元の端末10A-1の動作について説明する。

【0042】図2は端末10A-1のハードウェアの主要部分を示す構成図である。

【0043】図2に示すように、端末10A-1は、演算処理を行うCPU (Central Processing Unit) 201と、データを記憶するための主記憶装置202および2次記憶装置203と、端末外部との間の通信を制御する通信アダプタ204と、これらを接続するバス205とから構成されており、通信アダプタ204を介して、通信回線206により、LAN-A (100A) と接続されている。

【0044】図3は端末10A-1の主記憶装置202の利用形態を示す説明図である。

【0045】図3に示すように、主記憶装置202上には、LAN-A (100A) で使用されている暗号アルゴリズムC1を用いたC1暗号化プログラム301およびC1復号化プログラム302と、送信すべきデータを振り分けるための振り分けプログラム303と、暗号プロトコル変換サーバ1 (30A)、暗号プロトコル変換サーバ2 (30B) から送信されたデータを、元のデータに復元するための復元プログラム304とが格納され、また、ワークエリア305が確保されている。

【0046】さらに、暗号通信の送受信時に使用する情報として、暗号プロトコル変換サーバ1 (30A) との間の暗号通信用の鍵KAA1 (306) および暗号用初期値(乱数)A1 (307) と、暗号プロトコル変換サーバ2 (30B) との間の暗号通信用の鍵KBA1 (308) および暗号用初期値(乱数)A2 (309) と、端末10A-1自身の端末識別子310と、暗号プロトコル変換サーバ1 (30A) のサーバ識別子311と、暗号プロトコル変換サーバ2 (30B) のサーバ識別子312とが格納されている。

【0047】図4は端末10A-1の送信処理手順を示すフローチャートである。

【0048】図4に示すように、端末10A-1は、暗号通信の送信要求が入力されると、まず、該送信要求と共に送信者が入力した送信先の端末の端末識別子（ここでは、端末10B-1の端末識別子）を、ワークエリア305に設定する（ステップ401）。

【0049】続いて、ステップ401でワークエリア305に設定した端末の端末識別子（ここでは、端末10B-1の端末識別子）に基づいて、送信先の端末が接続されたLAN（ここでは、LAN-B（100B））を判断する（ステップ402）。

【0050】続いて、C1暗号化プログラム301のバラメータとなる、暗号プロトコル変換サーバ1（30A）との間の暗号通信用の鍵KAA1（306）および暗号用初期値A1（307）をワークエリア305に設定する（ステップ403）。ここで、暗号用初期値A1（307）は、CBC（Cipher Block Chaining：暗号文ブロック連鎖）モードでの暗号化／復号化に使用する定数（乱数）である。なお、CBCモードについては後述する。

【0051】続いて、C1暗号化プログラム301のバラメータとなる、暗号プロトコル変換サーバ2（30B）との間の暗号通信用の鍵KBA1（308）および暗号用初期値A2（309）をワークエリア205に設定する（ステップ404）。暗号用初期値A2（309）の役割は、暗号用初期値A1（307）の役割と同様である。

【0052】続いて、予め作成されて2次記憶装置203上のファイルAに格納されている平文状態のデータであって、端末10B-1に送信すべきデータを、ワークエリア305にロードする（ステップ405）。

【0053】続いて、振り分けプログラム303を用いて、ステップ405でワークエリア305にロードしたデータを、2個の暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）に各々振り分けるための振り分け処理を行う（ステップ406）。

【0054】ここで、振り分けプログラム11による振り分け方法の具体例について、図5を用いて説明する。

【0055】図5に示す例では、元のデータdと任意の乱数a1に基づいて、排他的論理和を利用して、2個の暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）に各々振り分けるデータa、bを生成している。

【0056】詳しくは、まず、任意の乱数をa1に与え、d1とa1との間で排他的論理和を取った結果を、b1とする。続いて、b1をa2とし、d2とa2との間で排他的論理和を取った結果を、b2とする。同様な処理を行うと、d1～d10からなる元のデータdから、a1～a10からなるデータaと、b1～b10からなるデータbとが生成される。

【0057】このようにして生成されたデータa、bは、各々、その内容が搅乱されており、それ自体としては意味判別困難である。

【0058】なお、振り分け方法としては、この例に限らず、2個の暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）のいずれか一方において、平文状態のデータが盗まれた場合でも、該一方のデータだけでは意味判別困難であるような振り分け方法であればよい。

10 10 【0059】さて、図4に戻って、端末10A-1は、ステップ403で設定したバラメータをC1暗号化プログラム301に与えて、C1暗号化プログラム301を実行し、暗号プロトコル変換サーバ1（30A）に振り分けるデータ（ここでは、データa）をCBCモードで暗号化する（ステップ407）。

【0060】ここで、CBCモードでの暗号化について、図6を用いて説明する。

20 20 【0061】図6に示すように、CBCモードは、暗号強度を増加させるために、現在通常使用（ISOで標準化済み）されている暗号利用モードであり、暗号化された1データブロックを、次に暗号化する1データブロックに排他的論理和を取ることで絡ませて、次々と連鎖させて暗号化している手法である。ブロック型暗号の利用モードについては、「現代暗号論理」（電子通信学会）の64頁～76頁に記載されている。

30 30 【0062】再び、図4に戻って、端末10A-1は、ステップ404で設定したバラメータをC1暗号化プログラム301に与えて、C1暗号化プログラム301を実行し、暗号プロトコル変換サーバ2（30B）に振り分けるデータ（ここでは、データb）をCBCモードで暗号化する（ステップ408）。

【0063】続いて、暗号プロトコル変換サーバ1（30A）経由の暗号通信で使用するヘッダ情報を作成するための領域、および、暗号プロトコル変換サーバ2（30B）経由の暗号通信で使用するヘッダ情報を作成するための領域を、ワークエリア305に確保する（ステップ409）。

40 40 【0064】続いて、ステップ409で確保した領域に、図7に示す形式700に基づいて、ヘッダ情報を設定する（ステップ410）。具体的には、ステップ401でワークエリア305に設定した端末10B-1の端末識別子、送信元の端末である端末10A-1自身の端末識別子310、暗号プロトコル変換サーバ1（30A）のサーバ識別子311からなるヘッダ情報701（図7においては、各々、7010、7011、7012としている。）を、一方の領域に設定し、ステップ401でワークエリア305に設定した端末10B-1の端末識別子、送信元の端末である端末10A-1自身の端末識別子310、暗号プロトコル変換サーバ2（30B）のサーバ識別子312からなるヘッダ情報702

(図7においては、各々、7020, 7021, 7022としている。)を、もう一方の領域に設定する。

【0065】続いて、ステップ410で設定したヘッダ情報701を先頭に添付しながら、ステップ407で暗号化したデータを、ファイルA1に格納し、また、ステップ410で設定したヘッダ情報702を先頭に添付しながら、ステップ408で暗号化したデータを、ファイルA2に格納する(ステップ411)。

【0066】続いて、ファイルA内に未暗号化データが格納されているか否かを判定し(ステップ412)、格納されているならば、ステップ405～ステップ411を繰り返す。ただし、ヘッダ情報701, 702は、ファイルA1, A2の先頭にのみ添付するものとする。実際には、送信単位であるパケット単位でヘッダ情報が必要となるが、ここでは、説明を簡単にするために、送信単位がファイル単位であるものとする。

【0067】また、ファイルA内に未暗号化データが格納されていなければ、ファイルA1, A2を、各々、WAN110を介して、暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)に送信する(ステップ413)。

【0068】次に、暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)の動作について説明する。

【0069】図8は暗号プロトコル変換サーバ1(30A)のハードウェアの主要部分を示す構成図である。

【0070】図8に示すように、暗号プロトコル変換サーバ1(30A)は、演算処理を行うCPU801と、データを記憶するための主記憶装置802および2次記憶装置803と、暗号プロトコル変換サーバ外部との間の通信を制御する通信アダプタ804と、これらを接続するバス805とから構成されており、通信アダプタ804を介して、通信回線806により、第三機関AのLAN(120A)と接続されている。

【0071】なお、暗号プロトコル変換サーバ2(30B)のハードウェアの主要部分を示す構成図も、図8と同様である。

【0072】図9は暗号プロトコル変換サーバ1(30A)の主記憶装置802の利用形態を示す説明図である。

【0073】図9に示すように、主記憶装置802上には、LAN-A(100A)で使用されている暗号アルゴリズムC1を用いたC1暗号化プログラム901およびC1復号化プログラム902と、LAN-B(100B)で使用されている暗号アルゴリズムC2を用いたC2暗号化プログラム903およびC2復号化プログラム904とが格納され、また、ワークエリア905が確保されている。

【0074】さらに、暗号通信の送受信時に使用する情報として、端末10A-1～10A-mの各々との間の

暗号通信用の鍵が設定されている鍵エリアA(906)と、端末10B-1～10B-nの各々との間の暗号通信用の鍵が設定されている鍵エリアB(907)と、暗号用初期値A1(908)および暗号用初期値B1(909)とが格納されている。

【0075】実際には、鍵エリアA(906)には、端末10A-1～10A-mの端末識別子9061ごとに、対応する鍵9062が設定されている。また、鍵エリアB(907)には、端末10B-1～10B-nの端末識別子9071ごとに、対応する鍵9072が設定されている。ただし、安全性を考慮し、2個の鍵エリア906, 907に設定されている鍵は、全て、互いに異なるようとする。

【0076】また、暗号用初期値A1(908)は、端末10A-1の主記憶装置202上に格納されている暗号用初期値A1(307)と同じ値であり、暗号用初期値B1(909)は、図12を用いて後述するが、端末10B-1の主記憶装置1102上に格納されている暗号用初期値B1(1207)と同じ値である。

【0077】なお、暗号プロトコル変換サーバ2(30B)の主記憶装置802の利用形態を示す説明図も、図9と同様である。ただし、安全性を考慮し、暗号プロトコル変換サーバ2(30B)の主記憶装置802上に格納されている鍵は、全て、暗号プロトコル変換サーバ1(30A)の主記憶装置802上に格納されている鍵とは異なるようとする。

【0078】図10は暗号プロトコル変換サーバ1(30A)の暗号変換処理手順を示すフローチャートである。

【0079】なお、暗号プロトコル変換サーバ1(30A)において、LAN-A(100A)に接続された端末10A-1～10A-mのうちのいずれかの端末(ここでは、10A-1)から送信されたデータ(ここでは、ファイルA1)は、2次記憶装置803上に格納される。

【0080】図10に示すように、暗号プロトコル変換サーバ1(30A)は、まず、2次記憶装置803上に格納されているファイルA1内のヘッダ情報701から、送信先の端末である端末10B-1の端末識別子7010、および、送信元の端末である端末10A-1の端末識別子7011を読み出して、ワークエリア905に設定する(ステップ1001)。

【0081】続いて、ステップ1001で読み出した送信元の端末10A-1の端末識別子7011と鍵エリアA(906)に設定されている端末識別子9061とのマッチングを行うことにより、送信元の端末10A-1と暗号プロトコル変換サーバ1(30A)との間の暗号通信用の鍵KAA1を検索し、ワークエリア905に設定する(ステップ1002)。

【0082】続いて、ステップ1001で読み出した送

信先の端末10B-1の端末識別子7010と鍵エリアB(907)に設定されている端末識別子9071とのマッチングを行うことにより、送信元の端末10B-1と暗号プロトコル変換サーバ1(30A)との間の暗号通信用の鍵KAB1を検索し、ワークエリア905に設定する(ステップ1003)。

【0083】続いて、C1復号化プログラム902のパラメータとなる、ステップ1002で読み出した鍵KA A1および暗号用初期値A1(908)をワークエリア905に設定する(ステップ1004)。

【0084】続いて、C2暗号化プログラム903のパラメータとなる、ステップ1003で読み出した鍵KA B1および暗号用初期値B1(909)をワークエリア905に設定する(ステップ1005)。

【0085】続いて、ファイルA1内のデータを、ワークエリア905にロードする(ステップ1006)。

【0086】続いて、ステップ1006でロードしたファイルA1内のデータについて暗号変換処理を行う(ステップ1007)。

【0087】すなわち、まず、ステップ1006でロードしたデータを、先頭から1ブロックずつ、ステップ1004で設定したパラメータをC1復号化プログラム902に与えて、C1復号化プログラム902を実行して復号化し、さらに、ステップ1005で設定したパラメータをC2暗号化プログラム903に与えて、C2暗号化プログラム903を実行して再暗号化する。なお、再暗号化されたデータは、ワークエリア905上の元の位置に格納される。

【0088】ステップ1007の暗号変換処理を終了すると、ワークエリア905上に格納されているデータ(再暗号化されたデータ)を、ファイルB1に格納する(ステップ1008)。

【0089】続いて、ファイルA1内に未変換データが格納されているか否かを判定し(ステップ1009)、格納されているならば、ステップ1006～ステップ1008を繰り返す。

【0090】また、ファイルA1内に未変換データが格納されていなければ、ファイルB1を、WAN110を介して、LAN-B(100B)に接続された端末10B-1に送信する(ステップ1010)。

【0091】なお、暗号プロトコル変換サーバ2(30B)の暗号変換処理手順を示すフローチャートも、図10と同様である。すなわち、LAN-A(100A)に接続された端末10A-1から送信されたファイルA2を、ファイルB2に変換し、WAN110を介して、LAN-B(100B)に接続された端末10B-1に送信する。

【0092】次に、送信先の端末10B-1の動作について説明する。

【0093】図11は端末10B-1のハードウェアの

主要部分を示す構成図である。

【0094】図11に示すように、端末10B-1は、端末10A-1と同様に、演算処理を行うCPU1101と、データを記憶するための主記憶装置1102および2次記憶装置1103と、端末外部との間の通信を制御する通信アダプタ1104と、これらを接続するバス1105とから構成されており、通信アダプタ1104を介して、通信回線1106により、LAN-B(100B)と接続されている。

【0095】図12は端末10B-1の主記憶装置1102の利用形態を示す説明図である。

【0096】図12に示すように、主記憶装置1102上には、LAN-B(100B)で使用されている暗号アルゴリズムC2を用いたC2暗号化プログラム1201およびC2復号化プログラム1202と、送信すべきデータを振り分けるための振り分けプログラム1203と、暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)から送信されたデータを、元のデータに復元するための復元プログラム1204とが格納され、また、ワークエリア1205が確保されている。

【0097】さらに、暗号通信の送受信時に使用する情報として、暗号プロトコル変換サーバ1(30A)との間の暗号通信用の鍵KAB1(1206)および暗号用初期値(乱数)B1(1207)と、暗号プロトコル変換サーバ2(30B)との間の暗号通信用の鍵KBB1(1208)および暗号用初期値(乱数)B2(1209)と、端末10B-1自身の端末識別子1210と、暗号プロトコル変換サーバ1(30A)のサーバ識別子1211と、暗号プロトコル変換サーバ2(30B)のサーバ識別子1212とが格納されている。

【0098】図13は端末10B-1の受信処理手順を示すフローチャートである。

【0099】なお、端末10B-1において、暗号プロトコル変換サーバ1(30A)から送信されたファイル(ここでは、ファイルB1)、および、暗号プロトコル変換サーバ2(30B)から送信されたファイル(ここでは、ファイルB2)は、2次記憶装置1103上に格納される。

【0100】図13に示すように、端末10B-1は、ファイルB1、B2の受信を完了すると、まず、2次記憶装置1103上に格納されているファイルB1内のヘッダ情報701から、暗号プロトコル変換サーバのサーバ識別子(ここでは、暗号プロトコル変換サーバ1(30A)のサーバ識別子)7012を読み出して、ワークエリア1205に設定する(ステップ1301)。

【0101】続いて、ステップ1301でワークエリア1205に設定した暗号プロトコル変換サーバのサーバ識別子(ここでは、暗号プロトコル変換サーバ1(30A)のサーバ識別子)に基づいて、経由された暗号プロ

トコル変換サーバ（ここでは、暗号プロトコル変換サーバ1（30A））を判断する（ステップ1302）。
【0102】続いて、2次記憶装置1103上に格納されているファイルB2内のヘッダ情報702から、暗号プロトコル変換サーバのサーバ識別子（ここでは、暗号プロトコル変換サーバ2（30B）のサーバ識別子）7020を読み出して、ワークエリア1205に設定する（ステップ1303）。

【0103】続いて、ステップ1303でワークエリア1205に設定した暗号プロトコル変換サーバのサーバ識別子（ここでは、暗号プロトコル変換サーバ2（30B）のサーバ識別子）に基づいて、経由された暗号プロトコル変換サーバ（ここでは、暗号プロトコル変換サーバ2（30B））を判断する（ステップ1304）。

【0104】続いて、C2復号化プログラム1202のパラメータとなる、暗号プロトコル変換サーバ1（30A）との間の暗号通信用の鍵KAB1（1206）および暗号用初期値B1（1207）をワークエリア1205に設定する（ステップ1305）。

【0105】続いて、C2復号化プログラム1202のパラメータとなる、暗号プロトコル変換サーバ2（30B）との間の暗号通信用の鍵KB1（1208）および暗号用初期値B2（1209）をワークエリア1205に設定する（ステップ1306）。

【0106】続いて、2次記憶装置1103上のファイルB1に格納されている再暗号化データを、ワークエリア1205にロードし（ステップ1307）、2次記憶装置1103上のファイルB2に格納されている再暗号化データを、ワークエリア1205にロードする（ステップ1308）。なお、ステップ1307でロードする再暗号化データのデータ量と、ステップ1308でロードする再暗号化データのデータ量とは、同量である。

【0107】続いて、ステップ1305で設定したパラメータをC2復号化プログラム1202に与えて、C2復号化プログラム1202を実行し、ステップ1307でロードした再暗号化データを復号化する（ステップ1309）。

【0108】続いて、ステップ1306で設定したパラメータをC2復号化プログラム1202に与えて、C2復号化プログラム1202を実行し、ステップ1308でロードした再暗号化データを復号化する（ステップ1310）。

【0109】続いて、復元プログラム1204を用いて、ステップ1309およびステップ1310で復号化した2個のデータを、元のデータに復元するための復元処理を行う（ステップ1311）。

【0110】ここで、復元プログラム1204による復元方法の具体例について、図14を用いて説明する。

【0111】図14に示す例では、図5に示した振り分け方法に呼応して、暗号プロトコル変換サーバ1（30

A）を経由して受信したデータaと、暗号プロトコル変換サーバ2（30B）を経由して受信したデータbとの間で排他的論理和を先頭から順に取ることにより、データa、bを、元のデータdに復元している。

【0112】さて、図13に戻って、端末10B-1は、復元処理により復元されたデータ（平文）を、2次記憶装置1103上のファイルBに格納する（ステップ1312）。

【0113】続いて、ファイルB1、B2内に未復号化データが格納されているか否かを判定し（ステップ1313）、格納されているならば、ステップ1307～ステップ1312を繰り返す。

【0114】以上説明した動作により、送信先の端末10B-1において、ファイルB内に、送信元の端末10A-1が作成したデータが、判別可能な元の形式（平文）で格納されることとなり、端末10A-1から端末10B-1に対する暗号通信が完了した。

【0115】従って、本実施例の暗号通信システムによれば、暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）が、各々、分担して暗号変換処理を行うと共に、分担させるデータの振り分け方法に工夫を施しているので、振り分け方法が明らかになった場合で、かつ、暗号変換処理時の平文が、2個の暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）から同時に洩れた場合でない限り、端末10A-1が作成した元のデータ（平文）が第三者に盗まれることはなく、元のデータの盗難を困難にすることができます。

【0116】また、本実施例の暗号通信システムによれば、暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）が、各々、暗号変換処理において、1ブロックごとに、復号化および再暗号化を行っているので、同時に平文状態となるデータの量が1ブロックのみであることから、データが平文状態となる時間が短くなる。従って、平文状態のデータが洩れる可能性がある時間が短くなり、また、この時間に平文状態のデータが盗まれても、1ブロック分のデータのみが判明するだけで済む。一方、暗号変換処理において、全てのデータを復号化して平文状態のデータに戻した後、再暗号化する場合を考えてみると、データが平文状態となる時間が長くなるので、平文状態のデータが漏れる可能性がある時間が長くなり、この時間に平文状態のデータが盗まれると、より大量のデータが判明してしまう。

【0117】このように、暗号変換処理において、1ブロックずつ、復号化および再暗号化を行うことで、データが平文状態となる時間が短くなるので、安全性を増加させることができる。

【0118】なお、図1に示した例では、暗号プロトコル変換サーバ1（30A）、暗号プロトコル変換サーバ2（30B）が、各々、第三機関AのLAN120A、

第三機関BのLAN120Bに接続されるようにすることで、秘匿性がさらに増加するようとしているが、暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)が、共に、WAN110に接続されるようにしてよい。

【0119】また、以下に示すような様々な変形例も考えられる。

【0120】(変形例1) 変形例1は、振り分け方法を、図5に示した振り分け方法の代わりに、図18に示す振り分け方法とした例である。

【0121】図18に示す振り分け方法は、元のデータdの先頭から、1ブロックずつ交互に抽出することにより、暗号プロトコル変換サーバ1(30A)に送信するデータa、および、暗号プロトコル変換サーバ2(30B)に送信するデータbを生成するという方法である。

【0122】なお、復元方法は、データa、bを各々復号化した後、各データの先頭から1ブロックずつ交互に抽出し、連結すればよい。

【0123】図18に示した振り分け方法で生成した2個のデータa、bは、元のデータdの1/2のデータ量であるので、暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)間で負荷が分散されることとなる。

【0124】このように、暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)に振り分けるデータa、bの量が、元のデータdの量より小さくなると、暗号変換処理に関する負荷分散効果があり、従って、暗号変換処理が高速化されるという効果があるので、特に、大容量の暗号通信に有効となる。

【0125】ただし、図18に示した振り分け方法では、元のデータdに対するブロック単位での転置が行われるので、暗号変換処理時に、再暗号化前の平文状態のデータが、ブロック単位で意味のあるデータとなる。そこで、ブロック長を十分に短くし、ブロック単位での意味が判別困難になるようにすることが好ましい。ブロック長としては、例えば、慣用暗号の1ブロック長(64ビット)や、16ビット未満や、8ビット未満とすることでできる。16ビットは、1文字分の漢字コードに相当しているので、16ビット未満とすることで、意味判別が困難になる。また、8ビットは、1文字分の英数字コードに相当しているので、8ビット未満とすることで、意味判別が困難になる。

【0126】このように、ブロック長を十分に短くすると、暗号変換処理時に、平文状態のデータの意味判別が困難になり、安全性を増加させることができる。

【0127】(変形例2) 変形例2は、変形例1において、意味判別をさらに困難にするために、図18に示した振り分け方法による振り分けを行う前に、元のデータdの各ブロックを、ランダムに転置しておくものである。

【0128】例えば、元のデータdのブロック数がn個であるとすると、(n!-1)通りの転置方法が存在するので、できるだけランダムな転置を行うために、乱数表を使用するようにし、送信元の端末と送信先の端末とが、同じ乱数表を保持すればよい。

【0129】(変形例3) 図1に示した例は、2個の暗号プロトコル変換サーバが接続されているようとしているが、変形例3は、3個以上の暗号プロトコル変換サーバが接続されているようとするものである。

10 【0130】例えば、3個の暗号プロトコル変換サーバが接続されている場合は、図5に示した振り分け方法で生成した2個のデータa、bを、ほぼ均等に、3個の暗号プロトコル変換サーバに振り分けるようにすればよい。すなわち、例えば、データaの先頭から2/3、データaの残りの1/3およびデータbの先頭から1/3、データbの残りの2/3を、各々、3個の暗号プロトコル変換サーバに振り分けなければならない。

20 【0131】図5に示した振り分け方法で生成した2個のデータa、bは、元のデータdの2倍のデータ量であるので、3個以上の暗号プロトコル変換サーバが接続されている場合には、これらの暗号プロトコル変換サーバ間で負荷が分散されることとなる。

【0132】(変形例4) 変形例4は、変形例1において、3個以上の暗号プロトコル変換サーバが接続されているようとするものである。

【0133】例えば、3個の暗号プロトコル変換サーバが接続されている場合は、図18に示した振り分け方法で、元のデータdの先頭から、1ブロックずつ交互に抽出することにより、3個の暗号プロトコル変換サーバに各々送信する3個のデータを生成すればよい。

30 【0134】なお、図18に示した振り分け方法では、k個(≥3)の暗号プロトコル変換サーバが接続されている場合には、k個の暗号プロトコル変換サーバに各々送信されるk個のデータが生成され、これらk個のデータは、元のデータdの1/kのデータ量であるので、これらk個の暗号プロトコル変換サーバ間で負荷が分散されることとなる。

40 【0135】(変形例5) 変形例5は、図5に示した振り分け方法で、元のデータdからデータa、bを生成した後、さらに、同じ振り分け方法で、データaからデータa1、a2を生成し、データbからデータb1、b2を生成するようするものである。

【0136】この場合、例えば、暗号プロトコル変換サーバA(30A)には、データa1、b1を振り分け、暗号プロトコル変換サーバB(30B)には、データa2、b2を振り分けなければならない。

【0137】この場合には、暗号変換処理に関する負荷分散効果はなく、むしろ負荷が2倍に増大してしまう。しかしながら、4個の暗号プロトコル変換サーバが接続されているようすれば、負荷の増大を解消することができます。

でき、また、5個以上の暗号プロトコル変換サーバが接続されているようにすれば、負荷を分散させることができる。

【0138】(変形例6)図1に示した例は、LAN-A(100A)に接続された端末10A-1~10A-m、および、LAN-B(100B)に接続された端末10B-1~10B-nが、同プロック長のプロック型慣用暗号を使用するものとしているが、変形例6は、ストリーム暗号または公開鍵暗号を使用するようにするものである。

【0139】プロック型慣用暗号が、数十ビット以上の比較的長いデータプロックごとに暗号化/復号化する暗号であるのに対して、慣用暗号の一種であるストリーム暗号は、1ビットから数ビットの小データプロックごとに暗号化/復号化する暗号である。例えば、プロック型慣用暗号のうちのDES(Data Encryption Standard)暗号は、64ビットごとに暗号化/復号化する暗号であり、プロック型慣用暗号のうちのMulti2(Multi-Media Encryption Algorithm2)暗号は、64ビットごとに暗号化/復号化する暗号であり、ストリーム暗号のうちのバーナム暗号は、1ビットごとに暗号化/復号化する暗号である。

【0140】また、公開鍵暗号は、相当長いデータプロックごとに暗号化/復号化する暗号である。例えば、公開鍵暗号のうちのRSA暗号は、64ビット(=512ビット)ごとに暗号化/復号化する暗号である。

【0141】なお、DES暗号の詳細については、「現代暗号理論」(電子通信学会)の41頁~49頁に記載されており、RSA暗号の詳細については、「現代暗号理論」(電子通信学会)の105頁~123頁に記載されている。また、Multi2暗号の詳細については、「マルチメディア向け高速暗号アルゴリズムHisecurity-Multi2の開発と利用法」(電子通信学会、暗号と情報セキュリティジョイントワークショップ講演論文集)の167頁~173頁に記載されている。

【0142】例えば、LAN-A(100A)に接続された端末10A-1~10A-mが、バーナム暗号を使用し、LAN-B(100B)に接続された端末10B-1~10B-nが、DES暗号を使用している場合は、暗号変換処理において、バーナム暗号で1ビットずつ64ビットを復号化する度に、DES暗号で該64ビットを再暗号化すればよい。

【0143】また、例えば、LAN-A(100A)に接続された端末10A-1~10A-mが、RSA暗号を使用し、LAN-B(100B)に接続された端末10B-1~10B-nが、DES暗号を使用している場合は、暗号変換処理において、RSA暗号で64ビットを復号化する度に、DES暗号で該64ビットを64ビットずつ再暗号化すればよい。

【0144】また、例えば、LAN-A(100A)に

接続された端末10A-1~10A-mが、RSA暗号を使用し、LAN-B(100B)に接続された端末10B-1~10B-nが、バーナム暗号を使用している場合は、暗号変換処理において、RSA暗号で64ビットを復号化する度に、バーナム暗号で該64ビットを1ビットずつ再暗号化すればよい。

【0145】ところで、互いに異なる暗号を使用する異国の端末間で暗号通信を行いたい場合に、少なくとも一方の国が、法律的に暗号技術に関する輸出入規制を行っており、輸出規制を行っている国の端末で使用している暗号のアルゴリズムを、他国の暗号プロトコル変換サーバに備えることができないという状況が考えられる。例えば、上述した暗号プロトコル変換サーバ1(30A)、暗号プロトコル変換サーバ2(30B)の少なくとも一方が、輸出規制国外にある場合は、そのような暗号プロトコル変換サーバに、輸出規制国の端末で使用している暗号のアルゴリズムを備えることができない。

【0146】そこで、このような状況において、2国の端末間で暗号通信を行うことを可能とするためには、一般に、特定の1個の暗号のみを共通に使用することを、2国間で協定する方法が考えられる。このように、2国間で共通に使用される暗号を「中間暗号」と呼ぶ。

【0147】そこで、中間暗号の使用を協定した場合の実施例を、第2の実施例として、以下に説明する。

【0148】図15は第2の実施例の暗号通信システムの構成図である。

【0149】図15に示した暗号通信システムは、A国に属し、A国で使用されている暗号を使用するLAN-A(100A)と、B国に属し、B国で使用されている暗号を使用するLAN-B(100B)に各々接続されている任意の端末間で、暗号通信を行うためのものである。

【0150】この暗号通信は、A国に属する、WAN-A(110A)、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)と、B国に属する、WAN-B(110B)、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40B-2)を経由して行われる。

【0151】図15に示すように、LAN-A(100A)は、複数の端末10A-1~10A-mが接続されたローカルエリア・ネットワークであり、通信回線50を介して、A国内のWAN-A(110A)と接続されている。また、LAN-B(100B)は、複数の端末10B-1~10B-nが接続されたローカルエリア・ネットワークであり、通信回線52を介して、B国内のWAN-B(110B)と接続されている。また、A国内のWAN-A(110A)とB国内のWAN-B(110B)とが、通信回線51を介して接続されている。

【0152】A国内には、暗号プロトコル変換サーバA

1 (40A-1), 暗号プロトコル変換サーバA2 (40A-2) が設置されており、各々、暗号アルゴリズムC1および中間暗号の暗号アルゴリズムを備えている。また、暗号プロトコル変換サーバA1 (40A-1), 暗号プロトコル変換サーバA2 (40A-2) は、各々、第三機関A1のLAN (130A-1), 第三機関A2のLAN (130A-2) に属し、LAN (130A-1), LAN (130A-2) は、各々、通信回線53, 54を介して、WAN-A (110A) と接続されている。

【0153】また、B国内には、暗号プロトコル変換サーバB1 (40B-1), 暗号プロトコル変換サーバB2 (40B-2) が設置されており、各々、暗号のアルゴリズムC2および中間暗号のアルゴリズムを備えている。また、暗号プロトコル変換サーバB1 (40B-1), 暗号プロトコル変換サーバB2 (40B-2) は、各々、第三機関B1のLAN (130B-1), 第三機関B2のLAN (130B-2) に属し、LAN (130B-1), LAN (130B-2) は、各々、通信回線55, 56を介して、WAN-B (110B) と接続されている。

【0154】以下、LAN-A (100A) に接続された端末10A-1からLAN-B (100B) に接続された端末10B-1に対する暗号通信を例にして、上述した暗号通信システムとは異なる点を中心、暗号通信システムの詳細な動作について説明する。

【0155】端末10A-1のハードウェアの主要部分を示す構成図は、図2と同様であり、端末10B-1のハードウェアの主要部分を示す構成図は、図11と同様である。

【0156】また、端末10A-1の主記憶装置202の利用形態を示す説明図、および、端末10A-1の送信処理手順を示すフローチャートは、実質的には、図3および図4と同様である。

【0157】ただし、端末10A-1においては、上述した暗号通信システムにおける暗号プロトコル変換サーバ1 (30A) を暗号プロトコル変換サーバA1 (40A-1) とみなし、上述した暗号通信システムにおける暗号プロトコル変換サーバ2 (30B) を暗号プロトコル変換サーバA2 (40A-2) とみなすようにする。すなわち、端末10A-1は、端末10B-1に送信すべきデータを、暗号プロトコル変換サーバA1 (40A-1), 暗号プロトコル変換サーバA2 (40A-2) の各々に振り分け、暗号化して送信する。

【0158】また、端末10B-1の主記憶装置1102の利用形態を示す説明図、および、端末10B-1の送信処理手順を示すフローチャートは、実質的には、図12および図13と同様である。

【0159】ただし、端末10B-1においては、上述した暗号通信システムにおける暗号プロトコル変換サー

バ1 (30A) を暗号プロトコル変換サーバB1 (40B-1) とみなし、上述した暗号通信システムにおける暗号プロトコル変換サーバ2 (30B) を暗号プロトコル変換サーバB2 (40B-2) とみなすようにする。すなわち、端末10B-1は、暗号プロトコル変換サーバB1 (40B-1), 暗号プロトコル変換サーバB2 (40B-2) を各々経由して送信されたデータを、復号化して元のデータに復元する。

【0160】また、暗号プロトコル変換サーバA1 (40A-1) の構成図、暗号プロトコル変換サーバA2 (40A-2) の構成図、暗号プロトコル変換サーバB1 (40B-1) の構成図、暗号プロトコル変換サーバB2 (40B-2) の構成図は、図8と同様である。

【0161】図16は暗号プロトコル変換サーバA1 (40A-1) の主記憶装置802の利用形態を示す説明図である。

【0162】図16に示すように、主記憶装置802上には、LAN-A (100A) で使用されている暗号アルゴリズムC1を用いたC1暗号化プログラム1601

20 およびC1復号化プログラム1602と、中間暗号の暗号アルゴリズムを用いた中間暗号暗号化プログラム1603および中間暗号復号化プログラム1604とが格納され、また、ワークエリア1605が確保されている。

【0163】さらに、暗号通信の送受信時に使用する情報として、端末10A-1～10A-mの各々との間の暗号通信用の鍵が設定されている鍵エリア1606と、暗号プロトコル変換サーバB1 (40B-1) との間の暗号通信用の鍵1607と、暗号用初期値A1 (1608) とが格納されている。

30 【0164】実際には、鍵エリア1606には、端末10A-1～10A-mの端末識別子16061とともに、対応する鍵16062が設定されている。また、暗号用初期値A1 (1608) は、端末10A-1の主記憶装置202上に格納されている暗号用初期値A1 (307) と同じ値である。

【0165】なお、暗号プロトコル変換サーバA2 (40A-2) の主記憶装置802の利用形態を示す説明図も、図16と同様である。ただし、暗号プロトコル変換サーバB1 (40B-1) との間の暗号通信用の鍵の代わりに、暗号プロトコル変換サーバB2 (40B-2) との間の暗号通信用の鍵が格納されている。

【0166】図17は暗号プロトコル変換サーバB1 (40B-1) の主記憶装置802の利用形態を示す説明図である。

【0167】図17に示すように、主記憶装置802上には、LAN-B (100B) で使用されている暗号アルゴリズムC2を用いたC2暗号化プログラム1701およびC2復号化プログラム1702と、中間暗号の暗号アルゴリズムを用いた中間暗号暗号化プログラム1703および中間暗号復号化プログラム1704とが格納

され、また、ワークエリア1705が確保されている。
【0168】さらに、暗号通信の送受信時に使用する情報として、端末10B-1～10B-nの各々との間の暗号通信用の鍵が設定されている鍵エリア1706と、暗号プロトコル変換サーバA1(40A-1)との間の暗号通信用の鍵1707と、暗号用初期値B1(1708)とが格納されている。

【0169】実際には、鍵エリア1706には、端末10B-1～10B-nの端末識別子17061ごとに、対応する鍵17062が設定されている。また、暗号用初期値B1(1708)は、端末10B-1の主記憶装置1102上に格納されている暗号用初期値B1(1107)と同じ値である。

【0170】なお、暗号プロトコル変換サーバB2(40B-2)の主記憶装置801の利用形態を示す説明図も、図17と同様である。ただし、暗号プロトコル変換サーバA1(40A-1)との間の暗号通信用の鍵の代わりに、暗号プロトコル変換サーバA2(40A-2)との間の暗号通信用の鍵が格納されている。

【0171】また、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)の暗号変換処理手順は、実質的には、図10と同様である。

【0172】ただし、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)は、暗号変換処理において、C1復号化プログラム902による復号化を行い、C2暗号化プログラム903による再暗号化を行う代わりに、C1復号化プログラム1602による復号化を行い、中間暗号暗号化プログラム1603による再暗号化を行うようにする。また、暗号プロトコル変換サーバA1(40A-1)は、再暗号化データを格納したファイルを、暗号プロトコル変換サーバB1(40B-1)に送信するようにし、暗号プロトコル変換サーバA2(40A-2)は、再暗号化データを格納したファイルを、暗号プロトコル変換サーバB2(40B-2)に送信するようにする。

【0173】なお、ここでは、暗号プロトコル変換サーバA1(40A-1)と暗号プロトコル変換サーバB1(40B-1)との間で中間暗号を使用した暗号通信を行い、暗号プロトコル変換サーバA2(40A-2)と暗号プロトコル変換サーバB2(40B-2)との間で中間暗号を使用した暗号通信を行うようにしているが、1個の暗号プロトコル変換サーバに重複して送信されないようになっていればよい。

【0174】また、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40B-2)の暗号変換処理手順も、実質的には、図10と同様である。

【0175】ただし、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40

B-2)は、暗号変換処理において、C1復号化プログラム902による復号化を行い、C2暗号化プログラム903による再暗号化を行う代わりに、中間暗号復号化プログラム1704による復号化を行い、C2暗号化プログラム1701による再暗号化を行うようにする。

【0176】このように、中間暗号の使用を協定した場合には、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)は、各々、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40B-2)との間の暗号通信用の鍵1607、および、LAN-A(100A)に接続された端末10A-1～10A-mの各々との間の暗号通信用の鍵16062を保持すればよく、LAN-B(100B)に接続された端末10B-1～10B-nの各々との間の暗号通信用の鍵17062を保持する必要はない。また、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40B-2)も、各々、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)との間の暗号通信用の鍵1707、および、LAN-B(100B)に接続された端末10B-1～10B-nの各々との間の暗号通信用の鍵17062を保持すればよく、LAN-A(100A)に接続された端末10A-1～10A-mの各々との間の暗号通信用の鍵16062を保持する必要はない。

【0177】従って、自国で使用している暗号のアルゴリズムを他国に属する暗号プロトコル変換サーバに備えなくても、暗号通信を行うことができる。

【0178】なお、図15に示した例では、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)が、各々、第三機関A1のLAN(130A-1)、第三機関A2のLAN(130A-2)に接続されるようにし、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40B-2)が、各々、第三機関B1のLAN(130B-1)、第三機関B2のLAN(130B-2)に接続されるようにすることで、秘匿性がさらに増加するようにしているが、暗号プロトコル変換サーバA1(40A-1)、暗号プロトコル変換サーバA2(40A-2)が、共に、WAN-A(110A)に接続されるようにし、暗号プロトコル変換サーバB1(40B-1)、暗号プロトコル変換サーバB2(40B-2)が、共に、WAN-B(110B)に接続されるようにしてもよい。

【0179】なお、中間暗号の使用を協定した場合でも、上述と同様な変形例が考えられる。
【0180】すなわち、上述した変形例1と同様に、振り分け方法を、図5に示した振り分け方法の代わりに、図18に示す振り分け方法とすることができる。

【0181】また、上述した変形例2と同様に、図18

に示した振り分け方法による振り分けを行う前に、元のデータdの各ブロックを、ランダムに転置しておくことができる。

【0182】また、上述した変形例3と同様に、A国に属する暗号プロトコル変換サーバ、および、B国に属する暗号プロトコル変換サーバが、各々、3個以上接続されているようにすることができる。

【0183】また、上述した変形例4と同様に、変形例1においても、A国に属する暗号プロトコル変換サーバ、および、B国に属する暗号プロトコル変換サーバが、各々、3個以上接続されているようにすることができる。

【0184】また、上述した変形例5と同様に、図5に示した振り分け方法で、元のデータdからデータa、bを生成した後、さらに、同じ振り分け方法で、データaからデータa₁、a₂を生成し、データbからデータb₁、b₂を生成するようにすることができる。

【0185】また、上述した変形例6と同様に、LAN-A(100A)に接続された端末10A-1~10A-m、および、LAN-B(100B)に接続された端末10B-1~10B-nが、ストリーム暗号または公開鍵暗号を使用するようにすることができる。

【0186】

【発明の効果】以上説明したように、本発明の暗号通信システムにおいては、送信元の端末が、送信すべきデータから、平文状態で意味判別困難な複数のデータを生成し、生成した複数のデータを暗号化してから複数の暗号プロトコル変換サーバに振り分けて送信するようにしているので、複数の暗号プロトコル変換サーバが暗号変換処理を分担して行うようにすることができ、さらに、各暗号プロトコル変換サーバが、一定のデータ量ごとに暗号変換処理を行うようにすることもできるので、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能となる。

【0187】また、送信元の端末が、送信すべきデータから、該データのデータ量よりデータ量が小さい複数のデータを生成するようにすれば、複数の暗号プロトコル変換サーバ間で負荷が分散され、各暗号プロトコル変換サーバが行う暗号変換処理の負荷が軽減されるので、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、高速に行うことが可能となる。

【0188】さらに、互いに異なる暗号を使用する端末が異なる国に属する場合でも、これらの国が共通に使用するよう協定した1個の暗号を利用し、これらの端末間で送受信されるデータが、国境を越えるときに、該協定した暗号で暗号化された状態となるようにすれば、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能となる。

【図面の簡単な説明】

【図1】第1の実施例の暗号通信システムの構成図。

【図2】送信元の端末のハードウェアの主要部分を示す構成図。

【図3】送信元の端末の主記憶装置の利用形態を示す説明図。

【図4】送信元の端末の送信処理手順を示すフローチャート。

【図5】振り分けプログラムによる振り分け方法の具体例を示す説明図。

【図6】CBCモードでの暗号化を示す説明図。

【図7】ヘッダ情報の形式を示す説明図。

【図8】暗号プロトコル変換サーバのハードウェアの主要部分を示す構成図。

【図9】暗号プロトコル変換サーバの主記憶装置の利用形態を示す説明図。

【図10】暗号プロトコル変換サーバの暗号変換処理手順を示すフローチャート。

【図11】送信先の端末のハードウェアの主要部分を示す構成図。

【図12】送信先の端末の主記憶装置の利用形態を示す説明図。

【図13】送信先の端末の受信処理手順を示すフローチャート。

【図14】復元プログラムによる復元方法の具体例を示す説明図。

【図15】第2の実施例の暗号通信システムの構成図。

【図16】A国内の暗号プロトコル変換サーバの主記憶装置の利用形態を示す説明図。

【図17】B国内の暗号プロトコル変換サーバの主記憶装置の利用形態を示す説明図。

【図18】振り分けプログラムによる振り分け方法の他の具体例を示す説明図。

【符号の説明】

100A…LAN-A、100B…LAN-B、10A

-1~10A-m…LAN-Aに接続された端末、10

B-1~10B-n…LAN-Bに接続された端末、1

1…振り分けプログラム、12、31A、31B…暗号

アルゴリズムC1、13、32A、32B…暗号アルゴ

リズムC2、14…復元プログラム、30A…暗号プロ

トコル変換サーバ1、30B…暗号プロトコル変換サー

バ2、110…WAN、120A…第三機関AのLAN

、120B…第三機関BのLAN、40A-1、40

A-2…A国内の暗号プロトコル変換サーバ、40B-

1、40B-2…B国内の暗号プロトコル変換サーバ、

110A…A国内のWAN-A、110B…B国内のW

AN-B、130A-1、130A-2…A国内の第三

機関のLAN、130B-1、130B-2…B国内の第三

機関のLAN、201、801、1101…CP

U、202、802、1102…主記憶装置、203、

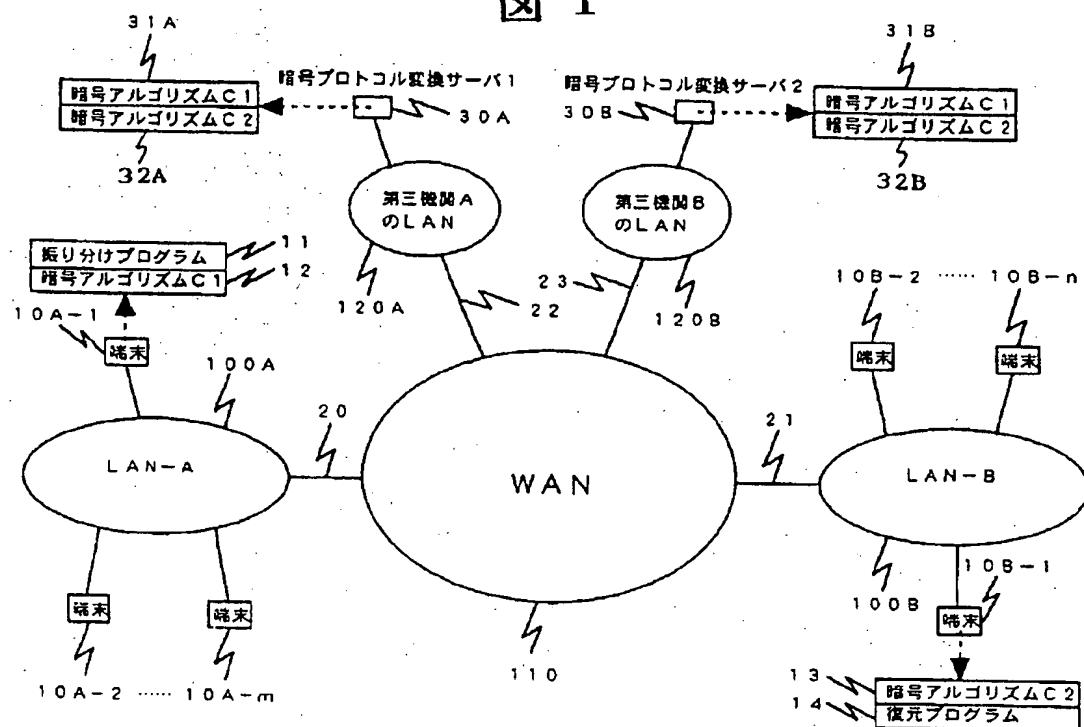
803、1103…2次記憶装置、204、804、1

104…通信アダプタ、205、805、1105…バ

ス。

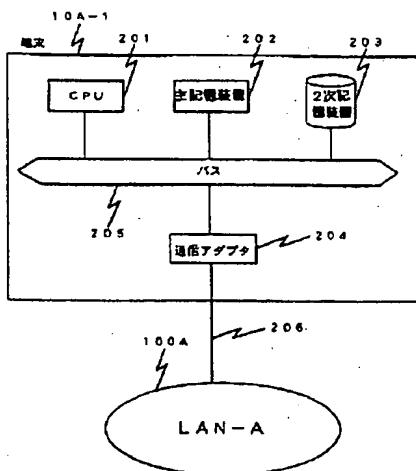
【図1】

図1



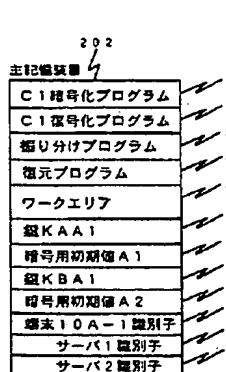
【図2】

図2



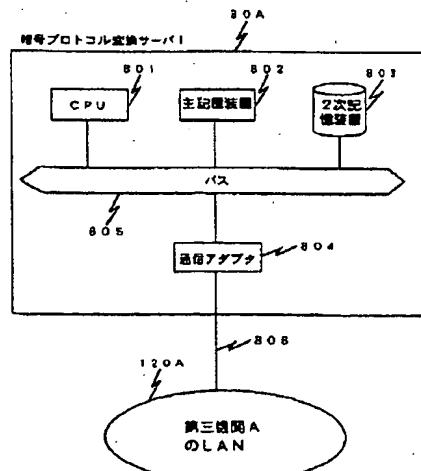
【図3】

図3



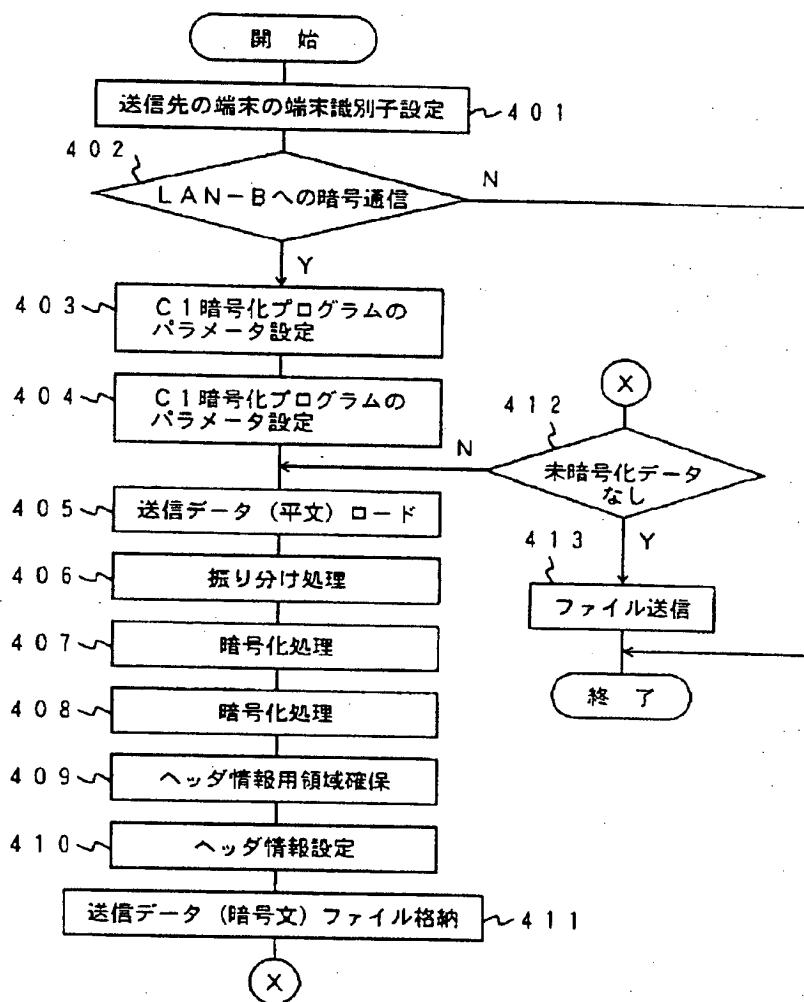
【図8】

図8



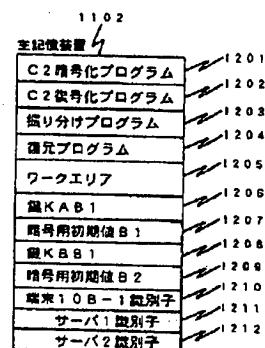
【図4】

図 4



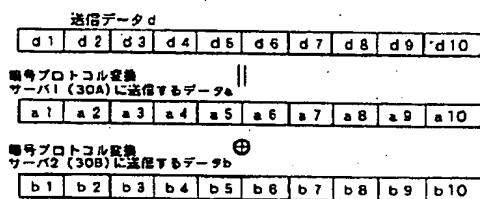
【図12】

図12



【図5】

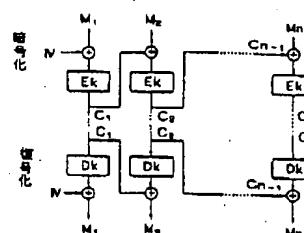
図5

データ a , b の生成方法の例

- (1) a_1 には、任意の乱数を与える
- (2) $a_1 = d_1 \oplus a_1$
- (3) $a_2 = b_1, a_2 = d_2 \oplus a_2$
- (4) $a(i) = b(i-1), b(i) = d(i) \oplus a(i) \quad (3 \leq i \leq 10)$

【図6】

図6

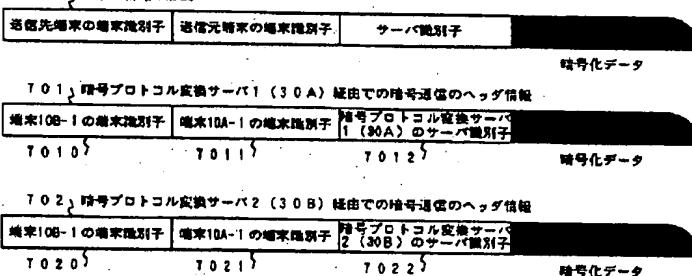


$M(i) \quad (1 \leq i \leq n)$: 平文系列
 $C(i) \quad (1 \leq i \leq n)$: 平文系列 $M(i)$ に対する暗号文系列
 $I \vee$: 初期定数
 E_k : 暗号鍵 k を用いた暗号化函数
 D_k : 暗号鍵 k を用いた復号化函数
 $C(1) = E_k(M(1) \oplus I \vee)$
 $C(i) = E_k(M(i) \oplus C(i-1)) \quad (2 \leq i \leq n)$
 $M(1) = D_k(C(1)) \oplus I \vee$
 $M(i) = D_k(C(i)) \oplus C(i-1) \quad (2 \leq i \leq n)$

【図7】

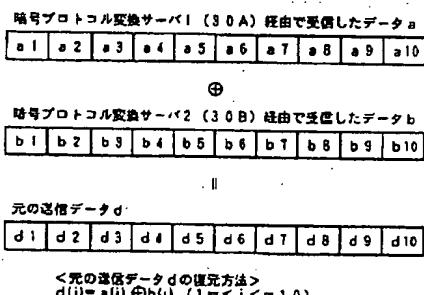
図7

100 ヘッダ情報の形式



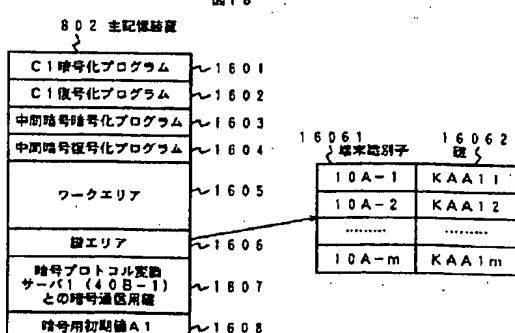
【図14】

図14



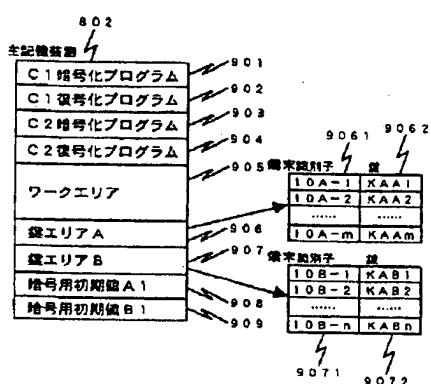
【図16】

図16



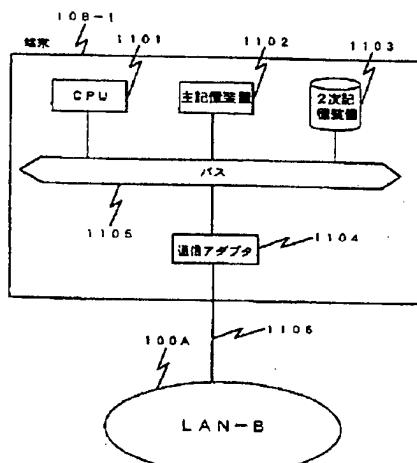
【図9】

図9



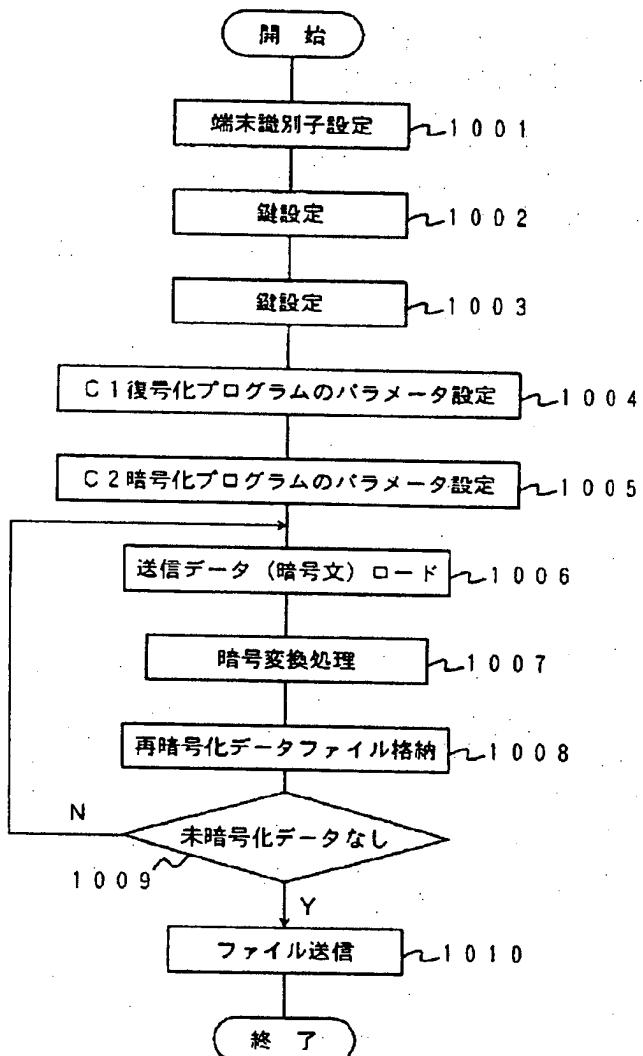
【図11】

図11



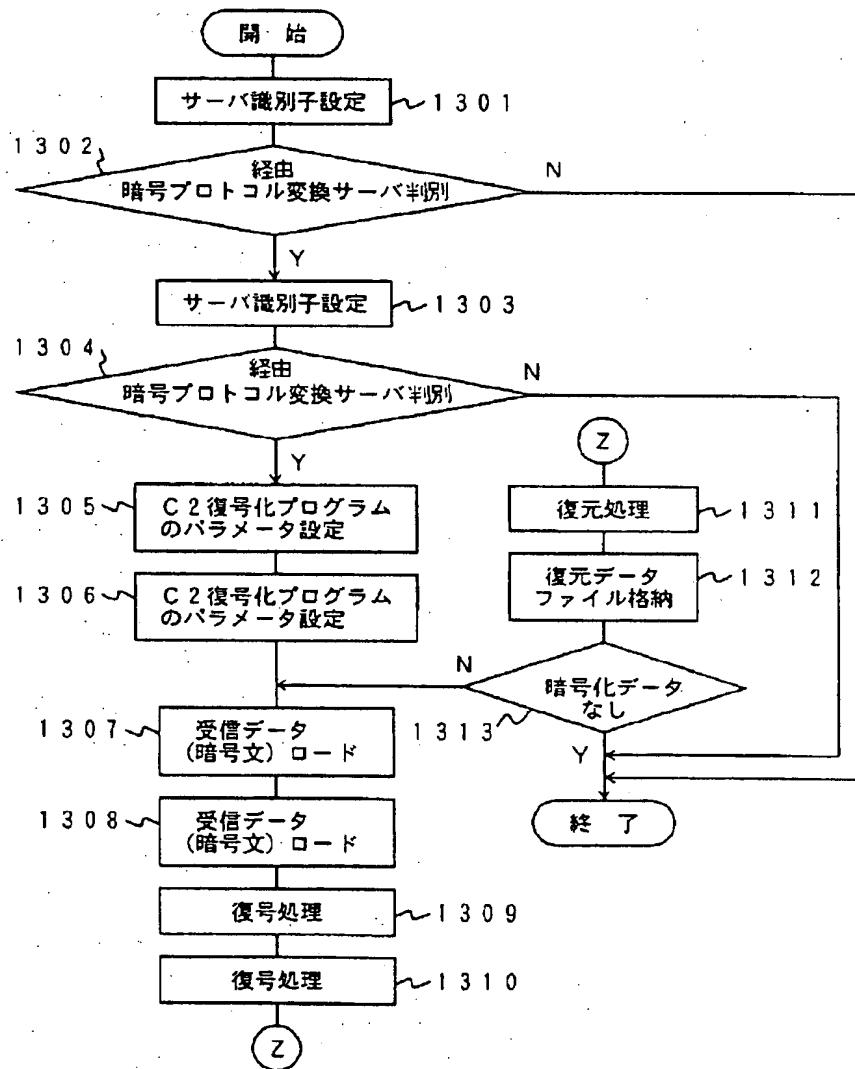
【図10】

図10



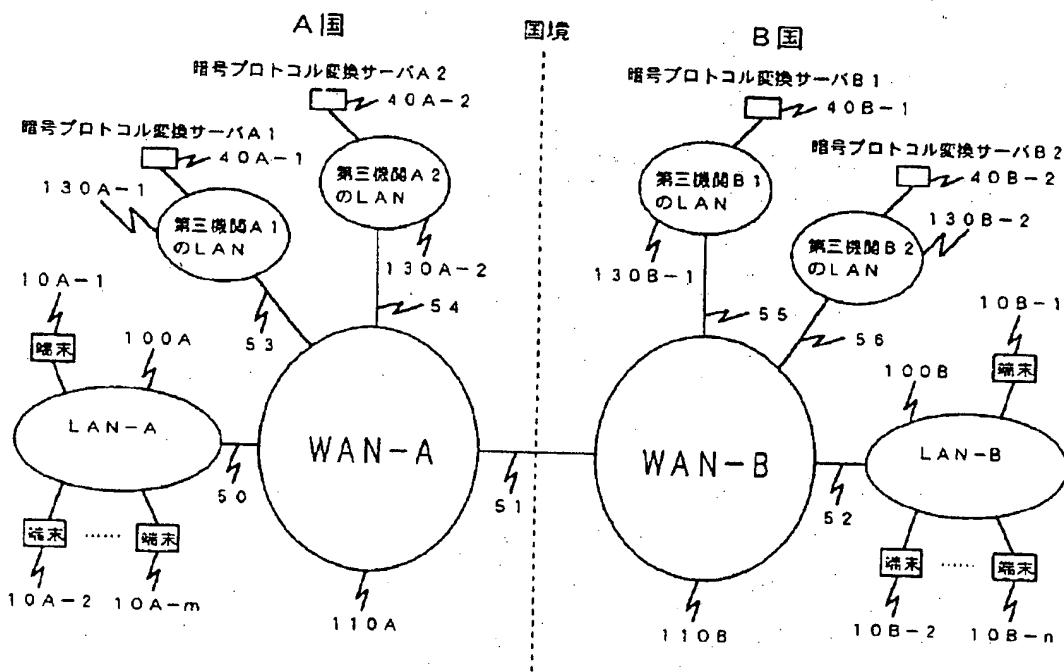
【図13】

図13



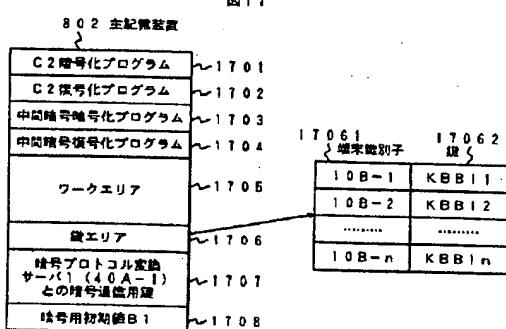
【図15】

図15



【図17】

図17



【図18】

図18

